www.flacsoandes.edu.ec

44

2011

Ciudad Segura

PROGRAMA ESTUDIOS DE LA CIUDAD FLACSO - ECUADOR

El hábil delincuente

Jaime Erazo Espinosa

Hace tiempos ya, un muy pensado enredo entre sistemas y aparatos informáticos y de comunicación con un específico conjunto de actividades estatales, de gobierno, de mercado y sociedad, iniciaron un espacio y mundo nuevo y virtual que hoy lo conocemos como cibernético y digital; a partir de su origen, se aceleró el desplazamiento y la interacción de no tan sólo lo material puntual sino de lo general, progresando también y por un lado, la institucionalización cada vez más sofisticada de nuevos ambientes imaginados, y por otro, la caracterización global de sus efectos como son la inmediatez y la imposibilidad de enfoques exactos. El nuevo y virtual espacio y mundo es acelerado, su velocidad desestabiliza órdenes establecidos y crea, entre variadas formas, u oportunidades tan simples o tan complejas como el "email" o Facebook, o comportamientos tan perturbadores como los violentos.

Ante él hay un espectro de inquietudes e incapacidades públicas, privadas e individuales: unas con respecto a su desarrollo, otras con respecto a su uso y ambas con respecto a su gobernanza. Las primeras tienen correlación con los sistemas educativos e investigativos que en países como Bolivia, Ecuador, Honduras, Nicaragua, Paraguay y Venezuela, son pobres; las segundas con la estructura jurídica, nacional y compartida a nivel internacional, de principios, normas, reglamentos y procedimientos de control y regulación; y las terceras con los marcos políticos que dictaminan las prioridades y las eficiencias de sus, por ejemplo, programas tanto de acceso universal como de competitividad.

Dentro del ciberespacio/mundo digital, su tecnología constitutiva complejiza y problematiza la seguridad, facilita el cometimiento de delitos, dificulta la prevención, detección y procesamiento de los mismos y, por tener alcance global, la persecución de los mentores/hacedores de ilícitos informáticos se asemeja a sus mismos ataques, es decir, a procesos sin discreción alguna. Así, la violencia dentro de lo virtual ha aumentado de nivel y se ha generado, sin limites, en cualquier parte del mundo convencional; sus condiciones, mecanismos y estrategias se comparten y protegen con el anonimato de quienes las generan. Y es que estos ciber y hábiles delincuentes, generadores de delitos informáticos, actúan violentando la información primada y privada de cualquiera (identidades, contraseñas, números de tarjetas y cuentas) para luego usarla en la confección de ilícitos concretos, entre los cuales tenemos: accesos, desvíos y apoderamientos ilegales (ej.: *wa r dali ng*); fraudes, daños y sabotajes financieros (ej.: *phi shi ng* o *pha rmi ng*); acosos y abusos a infantes y adolescentes (ej.: *sexti ng, groomi ng* o *bullyi ng*); ataques a infraestructuras de gobiernos y organizaciones (ej.: *hacki ng*); extorsiones y suplantaciones (ej.: *spoofi ng*); etc. Un ilícito virtual involucra siempre sistemas y aparatos informáticos o de comunicación: la Internet es la red electrónica que por su estructura tecnológica más ha permitido acoger a quebrantadores de la privacidad individual, junto a ella, la piratería ha producido millones de dólares en pérdidas en países tan dispares como México y Paraguay, el primero ocupó en 2009, el dieciseisavo lugar en tasa de piratería en América Latina (59%) y el segundo en pérdidas dentro de la misma región ($823 millones); por el contrario, el segundo en el mismo año, ocupó el segundo lugar en tasa (83%) y el dieciseisavo en pérdidas ($16 millones). Tanto la irrupción en la seguridad personal como el robo de derechos de autor ya están tipificados como delitos en los marcos jurídicos de nuestros países, cuando ellos son realizados en el ciberespacio/mundo digital, se los considera como variaciones de tipo y su penalización depende, primero de que haya norma y segundo, del mayor o menor rol de la tecnología en el incurrimiento del crimen electrónico.

Lo virtual y sus canales, ni son confiables ni son honestos, y aunque por derecho constitucional o leyes orgánicas –como la de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ecuador, 2002) o la 26.388 de Delitos Informáticos (Argentina, 2008)–, todo ciudadano tiene el privilegio de proteger sus datos personales cuando usa sistemas o aparatos informáticos o de comunicación, las infraestructuras digitales de nuestros países no son seguras (con rigurosos estándares) y no son privadas (exceptuando las intervenciones públicas de inteligencia). Por el contrario, las precauciones de los usuarios primero y después las de los desarrolladores, son medidas espontáneas que pretenden, sin sacrificar la privacidad, garantizar una segura convivencia ciudadana en el ciberespacio

FLACSO ECUADOR

TEMA CENTRAL

Seguridad ciudadana en el ciberespacio

Enrique Mafla[1]

Introducción

El ciberespacio constituye un nuevo ambiente de interacción social. La Constitución del Ecuador y varias leyes –entre las cuales la principal es la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos–, establecen los deberes y derechos de las personas naturales y jurídicas y tipifican las diferentes infracciones y delitos que pueden ocurrir dentro del ciberespacio. La seguridad del ciberespacio debe ser responsabilidad de todos los interesados: Estado, empresa privada y ciudadanos.

En los últimos años, la penetración de las tecnologías sobre las cuales se construye el ciberespacio se ha acelerado dramáticamente, lo cual ha traído consigo un aumento en el nivel de violencia en el mundo digital. Según el sitio *web* de la Superintendencia de Telecomunicaciones,[2] en abril de 2011, en el Ecuador habían 15'423.870 líneas activas del servicio móvil avanzado y 1.900 cibercafés registrados (el número de cibercafés informales, no registrados, debe ser mucho mayor). Según la misma fuente, en diciembre de 2010 había 3'097.315 usuarios de Internet; y en febrero de 2011, el número de usuarios y de enlaces de las empresas que prestan servicios de telecomunicaciones era 291.753 y 330.818, respectivamente. Ante el auge de los fraudes informáticos en el país, la Fiscalía General del Estado y la Su-perintendencia de Bancos y Seguros firmaron, el 21 de mar-zo de 2011, una resolución que obligaba a las instituciones financieras a devolver el dinero a más de 2.000 clientes afectados por delitos informáticos, aduciendo falta de seguridades informáticas en estas instituciones. Adicionalmente, la mencionada resolución obligó a las instituciones del sistema financiero a realizar campañas de información personalizada a los clientes y a emprender acciones correctivas para impedir el cometimiento de fraudes informáticos y delitos relacionados con el lavado de activos. Según las empresas GMS y Karspesky, los delitos informáticos crecieron un 360% entre 2009 y 2010.

Las actividades, trámites y transacciones que realizan los ciudadanos, las empresas y los Gobiernos se desplazan del mundo material al mundo digital cada vez con mayor celeridad. La seguridad convencional constituye una de las principales preocupaciones para los ciudadanos y para los Gobiernos nacionales y locales, a tal punto que fue la motivación principal para la realización del referendo y consulta popular del 7 de mayo de 2011. A la luz de las tendencias que acabamos de describir, estos actores deberían preocuparse también por la seguridad en el ciberespacio. El Programa Ciudad Segura de la FLACSO[3] plantea que la seguridad ciudadana en el mundo convencional constituye una problemática compleja que amerita una concepción integral. Esta problemática en el ciberespacio o mundo digital se complica aun más por las características de las tecnologías de información y comunicación (TIC) utilizadas para su construcción.

Primero, las TIC, y muy particularmente la Internet, han desestabilizado el orden establecido. Estas tecnologías han cambiado significativamente la forma en que las personas se comunican e interactúan. Desde el simple servicio de correo electrónico hasta las redes sociales (Facebook, Twitter, etc.) han creado nuevas y más complejas oportunidades de interacción social, pero al mismo tiempo han dado paso a nuevas formas de comportamientos violentos o antisociales. Estas nuevas formas de comportamiento social se desarrollaron cuando Internet empezó a salir de su ambiente puramente académico. Para tratar de normar el comportamiento de los ciudadanos en Internet, al inicio, aparecieron las reglas de etiqueta en la red.[4] Cuando estas reglas fueron insuficientes, los países empezaron a legislar y regular el comportamiento social de los ciudadanos conectados.[5] Esta última situación ha generado las mismas discusiones y preocupaciones que existen en el mundo convencional sobre el delicado dilema entre seguridad y privacidad (Smith, 2004; Schneier, 2010).

En segundo lugar, el efecto globalizador en el ciberespacio es inmediato. En el mundo virtual, la violencia puede ser generada desde cualquier parte del mundo. Existen atacantes autómatas maliciosos, tales como los *bots* –o robots de Internet– que pueden realizar ataques sin discreción a cualquier ciudadano del ciberespacio. Los ciber-delincuentes utilizan la Internet para compartir sus conocimientos, habilidades y herramientas delictivas y para formar asociaciones ilícitas globales.

Dada la complejidad de la problemática de la seguridad ciudadana en el ciberespacio, hemos establecido un alcance conceptual, geográfico, tecnológico y de profundidad en el análisis para este documento. Andreina Torres señala que

> existen diversas maneras de interpretar lo que la seguridad ciudadana es o debería ser, pudiendo ser definida de forma reduccionista, en base a modelos represivos, o de manera más amplia, llegando a colindar con el concepto de seguridad humana que envuelve todos los campos de la acción social (Torres, 2005).

Conceptualmente, el alcance de este documento estará apegado, más bien, a la primera de estas interpretaciones de la seguridad ciudadana.

El carácter global del ciberespacio dificulta realizar estudios enfocados a territorios geográficos específicos. Aunque muchos delitos informáticos involucran a ciudadanos que se conocen entre sí y que pueden vivir en la misma ciudad o país, la delincuencia informática tiende a trascender los límites locales, nacionales o regionales. Como ejemplo citaremos un delito que ha afectado a un gran número de ciudadanos: el robo de teléfonos móviles. Aunque éste no es un delito informático propiamente dicho, sí está relacionado al uso de las TIC para su control y litigación. La naturaleza globalizada de la telefonía móvil dificulta significativamente la

implementación de medidas efectivas para frenar este tipo de delincuencia. En el Ecuador, después de varios años de discusiones y acuerdos sobre este tema entre las autoridades y las empresas proveedoras del servicio de telefonía móvil, el 17 de mayo de 2011 comenzó a efectivizarse el control de teléfonos móviles robados. Por esta razón, no es posible limitar completamente el análisis de la seguridad ciudadana en el ciberespacio a límites geográficos.

En cuanto a las tecnologías que se utilizan en el ciberespacio, nuestro estudio se limita a las tecnologías de Internet. No consideraremos, en el presente documento, a pesar de su importancia y nivel de penetración en el país, a las tecnologías de telefonía móvil. Es necesario anotar que, aunque no existen estadísticas sobre esta convergencia, cada vez es mayor el número de abonados que utilizan sus teléfonos móviles para acceder a Internet. Finalmente, es necesario indicar que nuestro análisis estará limitado por la cantidad y calidad de los datos disponibles sobre esta problemática.

Considerando todos estos antecedentes, el objetivo del presente documento es describir y analizar, en términos generales, la problemática de la seguridad ciudadana en el ciberespacio. En las siguientes secciones, primero describiremos el ciberespacio desde el punto de vista de las tecnologías que utiliza, su desarrollo y su sistema de gobierno, y las implicaciones de estos aspectos sobre la seguridad ciudadana. Luego revisaremos la naturaleza y tipología de los delitos informáticos. A continuación analizaremos la problemática de la seguridad ciudadana en el Ecuador, para lo cual utilizaremos los pocos datos disponibles en el país sobre esta temática. Finalmente, presentaremos nuestras propuestas de solución para la construcción de un mundo digital seguro.

El ciberespacio y la brecha digital

"Ciberespacio" es un término que no tiene una definición precisa que sea ampliamente aceptada. Intuitivamente, al ciberespacio se lo concibe como el mundo virtual creado por las redes de computación y comunicación. La dificultad para definir el ciberespacio se debe, en gran medida, al desarrollo tecnológico. A partir del *hardware* (computadoras y redes de comunicación), el *software* va creando objetos virtuales cada vez más complejos. El archivo es uno de los primeros objetos virtuales que fue creado con *software*, cuando todavía no existían las redes de computadoras. La misma Internet (red de redes) es un espacio virtual fundamental creado con *software* especial (protocolos de comunicación). Sobre este espacio virtual fundamental se han ido creando espacios virtuales más sofisticados: la mensajería electrónica, la *web*, ambientes electrónicos distribuidos (e-gobierno, e-banca, e-educación, e-salud, etc.), redes sociales virtuales como Facebook, Twitter, etc.

Al inicio, estos espacios virtuales fueron adoptados por los ciudadanos sin que existiese una regulación formal sobre los mismos. Luego, se dio un proceso lento y no siempre acertado de incorporación de estos espacios virtuales de interacción social al marco jurídico de las instituciones y los países. En el Ecuador, esta situación se complica aun más debido principalmente a la brecha digital en materia de seguridad, la cual se mide a través de los siguientes parámetros: cultura de seguridad, conocimiento, infraestructura tecnológica segura y seguridad jurídica digital. A continuación realizaremos una breve descripción y análisis de estos parámetros, cuya comprensión es fundamental para desarrollar políticas públicas de seguridad ciudadana en el ciberespacio.

Las TIC reflejan la cultura, la cosmovisión y los valores de la sociedad que las produce. Internet es una tecnología que se desarrolló en el mundo académico de los Estados Unidos. Los protocolos de comunicación y las aplicaciones y servicios iniciales de esta red expresan los valores de ese mundo académico y, por tanto, el *software* básico de Internet no tiene controles explícitos de seguridad. La seguridad en la Internet original estaba basada en la confianza y la honestidad, especialmente académica, de los usuarios. Esta debilidad (falta de controles explícitos de seguridad) fue explotada fácilmente cuando la Internet empezó a utilizarse por las empresas privadas, los Gobiernos y la sociedad civil. Esta debilidad, que era bien conocida por los usuarios iniciales de Internet, es totalmente desconocida por la mayoría de usuarios de Internet en Ecuador. A esto debe sumarse la vulnerabilidad natural del ser humano a ser engañado. Kevin Mitnick, un ex ciber-delincuente muy conocido y actualmente consultor en seguridad informática, explica en su libro *El arte de la intrusión* (Mitnick y Simon, 2007), las técnicas más populares de ingeniería social –la explotación de las vulnerabilidades naturales del ser humano– utilizadas en Internet.

El segundo parámetro que mide la brecha digital es el conocimiento que los ciudadanos, las organizaciones y los Gobiernos tienen sobre seguridad informática. En Ecuador no existe ninguna carrera universitaria en la materia. En el mejor de los casos se dictan cursos marginales sobre aspectos tecnológicos de seguridad informática, ignorando los aspectos organizacionales, que son los más importantes. La gran mayoría de ciudadanos que usan Internet no ha recibido ninguna capacitación sobre los peligros que existen o sobre las consecuencias legales que puede ocasionar su uso indebido. Finalmente, tenemos la falta de conocimiento en los ejecutivos de las organizaciones, en los funcionarios de la función judicial y, lo que es más grave, en los legisladores. Los ejecutivos, judiciales y legisladores toman decisiones sobre el uso y gestión de las TIC –lo cual tiene un gran impacto sobre la seguridad en el ciberespacio– sin mayores fundamentos.

Pocas empresas privadas en el país exigen a sus ejecutivos formación y experiencia en gestión de tecnologías. La situación en el sector público es todavía más crítica. Los ejemplos sobre el mal uso y gestión de las TIC en este sector son innumerables. Como señalamos anteriormente, el Fiscal General del Estado acaba de ordenar a las instituciones financieras el resarcimiento a los perjudicados de los cada vez más frecuentes casos de fraudes informáticos financieros no como resultado de una investigación técnica, sino mediante una resolución entre la Fiscalía y la Superintendencia. Esta situación se da a pesar de que los bancos deben gestionar los riesgos tecnológicos de acuerdo a una resolución de la Superintendencia de Bancos (SBS, 2005). El Sistema Automático de Trámite Judicial Ecuatoriano (SATJE) ha tenido varios problemas de seguridad. El último incidente fue el relacionado con el uso de este sistema para el sorteo doloso de causas en la Función Judicial del Guayas.[6]

Así mismo, los sistemas TIC usados o contratados por el antes Tribunal Supremo Electoral y ahora Consejo Nacional Electoral han puesto varias veces en apuros a la democracia ecuatoriana. Uno de los casos más sonados fue el protagonizado por la empresa E-vote en el 2009. El jefe de la misión de observadores de la OEA, Enrique Correa, calificó de *desastrosa* a la falla del sistema informático en las elecciones presidenciales del 2009. Los desaciertos en el uso de la estadística y las TIC en los *exit polls* y en los conteos rápidos han afectado notablemente la credibilidad en estos valiosos instrumentos electorales. Los sistemas informáticos de la Corporación Aduanera Ecuatoriana, de la Policía de Migración, el IESS y de otras instituciones publicas también han sido mal usados en varias ocasiones.

El país carece de una infraestructura digital segura. La criptografía, en particular la criptografía de llave pública, es utilizada para implementar espacios virtuales seguros y confiables. Sin embargo, la confianza que se logre desarrollar entre los ciudadanos depende en gran medida de la construcción de la denominada infraestructura de llave publica (PKI por sus siglas en inglés). La raíz de confianza de esta infraestructura está en las autoridades que emiten los certificados digitales y en los entes de control. Los certificados digitales juegan en el mundo digital el rol de la cédula de identidad en el mundo físico. Las autoridades emisoras de certificados y los entes de control tienen el gran desafío de generar confianza entre los ciudadanos y demás actores del ciberespacio en los certificados digitales como medios seguros de identificación, autenticación y autorización.

El concepto de tiempo es tan importante en el mundo virtual como lo es en el mundo físico. El Ecuador todavía no dispone de los mecanismos tecnológicos y organizacionales que permitan marcar la hora virtual en el país. En particular, el país todavía no cuenta con ninguna autoridad de marcas de tiempo (TSA por sus siglas en ingles). De hecho, las marcas de tiempo emitidas por las TSA son inseguras y su integridad es incuestionable. La falta de TSA en el país ha ocasionado que se pusieran en duda ante los tribunales las horas en las que sucedieron dos eventos importantes del 30/S, pues no está claro la hora en que se realizó la firma electrónica del decreto presidencial que declaró el estado de emergencia o la del envío de los mensajes de correo electrónico a los medios de comunicación.[7]

Los graves problemas que genera en el país la inseguridad jurídica –y que han llevado a tomar medidas extremas como el referendo y consulta popular del pasado 7 de mayo– también se reproducen en el mundo virtual. Debido a los problemas que hemos descrito en los párrafos anteriores, la situación en el ciberespacio es todavía más crítica. La desesperanza y frustración de los ciudadanos por obtener justicia en los casos de fraude financiero han llevado a tomar la medida extrema de obligar a los bancos a devolver el dinero a los clientes perjudicados en todos los casos, es decir, sin analizar y procesar cada situación particular. La escasa y desactualizada normativa que existe en el país para regular la convivencia ciudadana en el ciberespacio no se cumple.

El *Reporte global sobre tecnologías de la información 2010-2011* (GITR), publicado por el Foro Económico Mundial y la Escuela de Negocios INSEAD (Dutta y Mia, 2011), confirma la magnitud de la brecha digital que acabamos de describir. De acuerdo al índice NRI (*Networked Readiness Index*), el Ecuador ocupa el puesto 108 entre los 138 países que fueron tomados en cuenta para la elaboración del GIRT. El mencionado índice mide, en una escala del 1 al 7, la capacidad del país (personas, empresas y Gobierno) para aprovechar las ventajas competitivas que ofrecen las TIC. Este índice resume el comportamiento de 71 variables y se calcula como el promedio aritmético de 3 subíndices, cuyos valores se calculan, a su vez, como el promedio de 3 pilares. Las 71 variables se distribuyen entre estos 9 pilares. La tabla 1 presenta los puestos que ocupa el Ecuador en el índice NRI, los subíndices y los pilares, conjuntamente con la nota correspondiente.

Los resultados de la tabla 1 ilustran claramente la brecha digital que separa al Ecuador del mundo desarrollado. Las peores calificaciones del país son las relacionadas al ambiente que ofrece el país para el efectivo aprovechamiento de las TIC y al nivel de preparación de las empresas y el Gobierno para aprovecharlas. El GITR resume, de manera clara y concisa, esta situación:

> Como en años anteriores, Honduras (103°), Ecuador (108°), Venezuela (119°), Paraguay (127°), Nicaragua (128°) y Bolivia (135°) se ubican por detrás del resto de la región y de la mayor parte de la muestra global. Estas economías comparten una serie de rasgos inquietantes que obstaculizan el desarrollo de la preparación para el uso de las TIC, incluyendo mercados sobre-regulados y marcos políticos ineficientes; pobres sistemas educativos y de investigación; escasos índices de penetración resultantes del limitado acceso a las TIC para la mayoría de la población, y, al final pero no con menor importancia, la poca prioridad dada a las TIC en los programas de gobierno y las estrategias de competitividad (Dutta y Mia, 2011, la traducción es nuestra).

La gobernanza de Internet

Las tecnologías utilizadas en Internet facilitan el cometimiento de delitos y dificulta su prevención, detección y procesamiento. Los delincuentes utilizan estas tecnologías para proteger su anonimato. El mismo FBI tiene serias dificultades para identificar, por medios tecnológicos, a los ciber-delincuentes, y debe recurrir a mecanismos tales como las recompensas para este propósito. Mientras los delincuentes poseen los conocimientos, las habilidades tecnológicas y el tiempo para actuar en su provecho, los encargados de administrar la seguridad en el ciberespacio no cuentan, por lo general, con las mismas condiciones.

Los delitos en el ciberespacio tienen un alcance geográfico global, lo cual dificulta enormemente la persecución de los delincuentes. Innumerables barreras jurídicas se interponen para llevar a los delincuentes ante la justicia, una vez que han sido identificados y localizados. Esta situación se da inclusive entre países que tienen una relación muy cercana entre sus instituciones judiciales. Uno de los casos más sonados, que ilustra esta situación, es el de Gary McKinnon, conocido también como *Solo*,[8] presunto ciber-delincuente cuya extradición desde el Reino unido está siendo tramitada por parte de los Estados Unidos desde el 2002. El juzgamiento de ciber-delincuentes identificados y localizados en países considerados como santuarios del ciber crimen es casi imposible.

A estos problemas de seguridad se debe sumar los problemas relacionados al respecto de los denominados *derechos digitales*. Estos derechos definen los privilegios que deberían tener los ciudadanos para usar los computadores y las redes, tales como el derecho a la privacidad de las

Tabla N.° 1. Resultados del Ecuador en el GITR 2010-2011

Ambiente para las TIC 117-3,18			Nivel de preparación 113-3,76			Uso de las TIC 98-2,83		
Mercado	Regulación	Infraestructura	Personas	Empresas	Gobierno	Personas	Empresas	Gobierno
127-3,38	116-3,36	100-2,81	82-4,72	123-3,30	123-3,27	89-2,94	109-2,61	99-2,94

comunicaciones, la libertad de expresión, la protección de los datos personales, la libertad de asociación, el derecho de acceso a las nuevas tecnologías, etc.

Para mitigar estos problemas, se ha planteado la necesidad de establecer un sistema de gobernanza de Internet. Lamentablemente, los Gobiernos, las corporaciones, los entes judiciales, la sociedad civil y los organismos internacionales como la ONU no han logrando mayores consensos sobre los mencionados temas. Existen posiciones política e ideológicamente antagónicas que van desde una total apertura y libertad en el uso, desarrollo y gobierno de Internet –como la de Internet Society–,[9] hasta el establecimiento de entes policíacos en el ciberespacio, pasando por propuestas académicas como el Proyecto de Gobernanza de Internet.[10]

El Foro sobre la Gobernanza de Internet[11] fue constituido por la ONU para facilitar la construcción de consensos entre los diferentes actores sobre estos temas. La constitución de este foro fue uno de los mandatos de la Cumbre Mundial sobre la Sociedad de la Información (WSIS), organizada por la ONU, que se llevó a cabo en dos fases: Ginebra (2003) y Túnez (2005). Un grupo de trabajo establecido por esta cumbre estableció la siguiente definición de *Governanza Internet:*[12]

> La gobernanza de Internet se refiere al desarrollo y la aplicación, por parte de los Gobiernos, el sector privado y la sociedad civil, en sus respectivas funciones, de principios, normas, reglamentaciones, procedimientos para toma de decisiones y programas compartidos que den forma a la evolución y el uso de Internet (la traducción es nuestra).

Yochai Benkler propone un marco de referencia de 3 capas para discutir sobre la gobernanza de Internet.[13] En primer lugar están las diferentes redes físicas que, interconectadas entre sí, conforman la infraestructura física de Internet. Estas redes pertenecen a diferentes organizaciones públicas y privadas, las cuales tienen total autonomía para administrarlas.

En la capa intermedia de este marco de referencia está la misma red Internet, la cual aparece ante los usuarios como una sola red que conecta a millones de computadoras. El *software* utilizado para construir la abstracción de una sola red (lógica) es el protocolo de comunicación IP (*Internet Protocol*), cuyos elementos principales son el sistema de direcciones y nombres, y el sistema de enrutamiento. Cada una de las computadoras conectadas a Internet tiene su propia dirección IP y muchas computadoras, especialmente las que actúan como servidores, tienen nombres (por ejemplo, www.flacso.edu.ec o www.cnn.com). La comunicación entre las computadoras se realiza en paquetes, es decir, las páginas *web*, los videos o las canciones que el usuario baja de un sitio de Internet son divididos en paquetes para su transmisión, los cuales son enrutados a través de las diferentes redes físicas que conforman la red.

La administración de estos elementos claves para el funcionamiento de Internet (direcciones, nombres y enrutamiento) ha pasado por varias manos. Primeramente fue administrada por el Departamento de Defensa de Estados Unidos, y luego por la Fundación Nacional para la Ciencias del mismo país. Cuando Internet salió del mundo académico y se privatizó y comercializó su uso, la administración pasó al Departamento de Comercio. Actualmente, Internet es administrada por una organización no gubernamental con sede en los Estados Unidos, cuyo nombre en español es Corporación Internet para Números y Nombres Asignados (ICANN). La importancia estratégica de las direcciones y nombres de Internet se ve claramente con lo sucedido a Wikileaks. Esta organización perdió su nombre oficial (www.wikileaks.org) e inclusive sus direcciones IP debido a sus enfrentamientos con el gobierno de los Estados Unidos.

Finalmente, tenemos la capa de contenidos. Este es el elemento más crítico y controversial en la discusión sobre la gobernanza de Internet, ya que en él están involucrados principios y derechos como la seguridad y la privacidad, la propiedad intelectual y el comercio internacional, la libertad de expresión, el acceso universal a la información y el conocimiento, la democratización de las TIC, etc.

El Ecuador no ha participado efectivamente en ninguna de las cumbres, foros o seminarios donde se ha discutido el presente y futuro de Internet. La falta de una política de Estado sobre el ciberespacio ha causado que, si bien algunos funcionarios del Gobierno, empresas y organizaciones no gubernamentales sí han asistido a esos eventos, lo hayan he-cho sin tener una idea clara sobre la posición del país en estos temas estratégicos.

Seguridad y privacidad en el ciberespacio

La seguridad y la privacidad en el ciberespacio han sido tratadas como un dilema inevitable entre estos dos derechos ciudadanos. Este dilema se acentuó a raíz del 11 de septiembre. A nombre de una mayor seguridad, el Gobierno de los Estados Unidos modificó y suprimió derechos sobre la confidencialidad de la información y la comunicación personal. Estas enmiendas no sólo afectan a los ciudadanos de ese país, sino que tienen un impacto sobre los derechos de los ciudadanos de otros países. Por ejemplo, como consecuencia de estos cambios legales, el FBI y otros cuerpos policiales y judiciales de los Estados Unidos tienen la potestad de, sin ninguna autorización previa, intervenir la información y comunicación de los ciudadanos que usan los diferentes servicios públicos de Internet, como Yahoo, Gmail, Hotmail y Facebook. Para lograr este objetivo, las empresas que brindan estos servicios deben implementar *puertas traseras* en sus infraestructuras tecnológicas para que aquellas fuerzas del orden puedan realizar las intervenciones que consideren necesarias con total libertad.

Bruce Schneier presenta argumentos en contra de este dilema.[14] Schneier afirma que no es necesario sacrificar la privacidad en el ciberespacio para fortalecer la seguridad. Varias medidas que han sido tomadas para supuestamente fortalecer la seguridad en el ciberespacio no solo que han afectado la privacidad de los ciudadanos, sino que han causado daño a la misma seguridad. Un ejemplo de este tipo de escenarios es el que ocurrió cuando supuestos ciber-delincuentes chinos aprovecharon las puertas traseras que utiliza el FBI para acceder a varios servicios de Internet,[15] afectando la seguridad de la información de millones de usuarios. Este problema trajo serias repercusiones que afectaron seriamente las relaciones entre Estados Unidos y China.

En el Ecuador, los problemas de la brecha digital que describimos anteriormente han complicado el tratamiento de este supuesto dilema. Nuestros legisladores han ido creando confusión sobre el asunto. Por un lado, la Constitución establece derechos sobre la privacidad de los datos personales y la inviolabilidad de las comunicaciones tanto en el mundo convencional como en el ciberespacio. Sin embargo, el 31 de marzo de 2010 fue publicada en el Registro Oficial la Ley del Sistema Nacional de Registro de Datos Públicos. Aunque varios artículos controversiales de esta ley fueron eliminados o modificados durante su tratamiento en la Asamblea Nacional, todavía existen inquietudes sobre su aplicación. La mencionada ley va en contracorriente con la tendencia que existe en la mayoría de países de privilegiar la privacidad de los datos personales a través de leyes orgáni-

cas. En España, por ejemplo, está vigente la Ley Orgánica de Protección de Datos de Carácter Personal. La Agencia Española de Protección de Datos, que funciona bajo esta ley, "vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal."[16]

Delitos informáticos

El delito informático es cualquier delito que involucre un computador o una red de comunicación. Estos delitos se clasifican de acuerdo al rol de la tecnología en el delito: como instrumento para el cometimiento del crimen o como objetivo del mismo. Entre los delitos más populares tenemos el acceso ilegal a computadores y redes, la violación de derechos de autor, la pornografía infantil, el robo de información confidencial, los fraudes financieros, el acoso y abuso de menores, el ataque a la infraestructura tecnológica de las organizaciones y países, el robo de identidades, etc.

En el Ecuador, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, así como su correspondiente reglamento, están vigentes desde el 17 de abril y el 31 de diciembre de 2002, respectivamente. Sin embargo, falta mucho por hacer para que esta ley proteja efectivamente los derechos de los ciudadanos y de la sociedad en el ciberespacio. La brecha digital que existe en la Función Judicial, la Policía Judicial y la Fiscalía impide que los ciudadanos se sientan protegidos y seguros en el ciberespacio. Todavía no existe un solo laboratorio de análisis forense que posibilite el procesamiento técnico y científico de los cada vez más frecuentes casos que se denuncian y tramitan en el sistema judicial. Prácticamente no existe personal especializado para investigar y procesar este tipo de delitos informáticos. Simples trámites como la notarización de documentos, eventos o sistemas electrónicos son imposibles de realizar. Los notarios que acudieron al Consejo Nacional Electoral y a las juntas intermedias y delegaciones provinciales electorales el 7 de mayo de 2011 no tenían el conocimiento, las herramientas ni los procedimientos para notarizar los elementos y eventos digitales sobre los que supuestamente debían dar fe, tales como la integridad y la autenticidad de los sistemas informáticos electorales o la inicialización en cero de la base de datos de los resultados electorales.

Ni la Fiscalía ni la Policía Judicial registran estadísticas confiables sobre los delitos informáticos. Ante el auge de los fraudes financieros que afectan a los clientes de los bancos, la Fiscalía ha comenzado a procesar estadísticas básicas sobre este tipo de delitos. La tabla 2 presenta los datos de la Fiscalía sobre delitos informáticos correspondientes al año 2010.

En Estados Unidos, el FBI, el Departamento de Justicia y el National White Collar Crime Center han conformado el Centro para Denuncias de Crímenes en Internet (IC3), cuyo fin es ayudar a las víctimas de crímenes en Internet en el procesamiento de las denuncias. El sitio web del IC3 (www.ic3.org) proporciona un mecanismo en línea para que los ciudadanos puedan formular sus denuncias. Así mismo, dispone de páginas que describen las principales tendencias y esquemas de los crímenes que se cometen en Internet, así como las correspondientes medidas de prevención. La mayor parte de esta información es válida para el Ecuador. Esta organización produce un reporte anual sobre crímenes en Internet con estadísticas muy detalladas.

Conclusiones y recomendaciones

La seguridad de los ciudadanos en el ciberespacio es una tarea pendiente en el Ecuador. Los problemas de inseguridad en Internet se han vuelto visibles en el último año, en particular en relación a los fraudes financieros. Estos hechos han desnudado los graves problemas de seguridad que tiene el ciberespacio en Ecuador. La solución de estos problemas pasa, en gran medida, por el acortamiento de la brecha digital, lo cual debe guiar la definición de las políticas publicas en esta área.

La seguridad no es intuitiva, y lo es mucho menos en ambientes como Internet, cuyas tecnologías y aplicaciones las importamos de otras culturas. Los bancos, por resolución de la Fiscalía y la Superintendencia de Bancos, han comenzado campañas de capacitación y concienciación ciudadana sobre seguridad en banca electrónica. La fundación Telefónica esta realizando un análisis sobre el uso de tecnologías interactivas entre los niños, adolescentes y jóvenes. Algunas empresas públicas y privadas han realizado programas de capacitación de seguridad informática para sus empleados. Sin embargo, estos esfuerzos aislados no son suficientes, y es necesario definir e implementar políticas de desarrollo de una cultura de seguridad digital que involucre a escuelas, colegios, universidades, hogares y organizaciones.

El marco regulatorio que norma la convivencia ciudadana en el ciberespacio es pobre y desactualizado. Únicamente el sistema financiero tiene una norma que dicta la forma en que las instituciones de este sistema deben gestionar las TIC. Los fraudes financieros que sufren los clientes de bancos y cooperativas de ahorro y crédito revelan claramente que esta normativa no es suficiente. Es indispensable que todos los sistemas públicos y privados, y no solo el sistema financiero, tengan regulaciones detalladas, actualizadas y especializadas para cada sector sobre la gestión de las TIC, para así garantizar los derechos ciudadanos en Internet.

El informe del GITR refleja objetivamente el atraso tecnológico del Ecuador con respecto al resto del mundo. La falta de capacidad para usar las TIC, especialmente en las empresas y el Gobierno, afecta gravemente la competitividad del país. Las variables utilizadas para el cálculo del NRI

Tabla N.° 2. Datos de la Fiscalía sobre delitos informáticos (2010)

Descripción 2009	Noticia de delito	Indagación previa	Desestimación	Inst. fiscal	Acusatorio	Absentivo	Sentencias condenatorias	Sentencias absolutorias
Daños informáticos de servicio público	86	86	0	0	0	0	0	0
Daños informáticos de servicio privado	163	163	0	2	0	0	0	0
Falsificación electrónica	23	15	10	1	0	0	0	0
Apropiación ilícita	168	117	37	13	10	1	0	0

desnudan la debilidad de la infraestructura tecnológica del país. En el futuro cercano, esta infraestructura tecnológica no solo deberá tener capacidades cada vez mayores de rendimiento (ancho de banda, procesamiento y almacenamiento), sino, y lo que es mas importante, deberá ser segura. En este campo, el país todavía no ha comenzado a caminar. Solo basta ver los duros reglamentos que la Unión Europea (UE) impone a las empresas de otros países sobre la gestión de la seguridad de la información para darse cuenta de los serios retos que tiene el país si desea participar en los procesos de integración. En particular, existe una regulación de la UE (Safe Harbor Framework)[17] que obliga a las empresas de otros países que desean mantener relaciones comerciales con la UE a cumplir con rigurosos estándares de seguridad informática que garanticen la protección de la información privada

Bibliografía

Dutta, Soumitra e Irene Mia (2011). *The Global Information Technology Report 2010–2011*. Foro Económico Mundial.

Mitnick, Kevin y William Simon (2007). *El arte de la intrusión*. Editorial Alfa Omega.

SBS (Superintendencia de Bancos y Seguros) (2005). "Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, Título VII, Subtítulo VI, Capítulo V: De la Gestión del Riesgo Operativo".

Schneier, Bruce (2010). *Young People, Privacy, and the Internet*. Disponible en http://www.schneier.com/blog/archives/2010/04/young_people_pr.html

Smith, Marcia (2004). *Internet Privacy: Overview and Pending Legislation*. The Library of Congress

Torres, Andreina (2005). *La seguridad ciudadana en Ecuador: un concepto en construcción*. Quito: FLACSO Ecuador/ Fundación Esquel.

Notas:

1 Profesor Principal, Escuela Politécnica Nacional
2 http://www.supertel.gob.ec
3 http://www.flacso.org.ec/html/boletinciudadsegura.html
4 http://www.rfc.org/rfc/rfc1855.html
5 http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
6 http://m.expreso.ec/ediciones/2011/02/11/nacional/actualidad/manipulacion-dolosa-en–sorteo-de-causas-de-la-corte/
7 http://www.monografias.com/trabajos82/ecuador-30-s-derecho/ecuador-30-s-derecho2.shtml
8 http://en.wikipedia.org/wiki/Gary_McKinnon
9 http://www.isoc.org/
10 http://www.internetgovernance.org/
11 http://www.intgovforum.org/cms/
12 http://www.wgig.org/docs/WGIGREPORT.pdf
13 http://www.law.indiana.edu/fclj/pubs/v52/no3/benkler1.pdf
14 http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html
15 http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/
16 http://www.aepd.es
17 http://www.export.gov/safeharbor/index.asp

COMPARANDO

Piratería de *software* en América Latina (mayo 2009)

Tasas de piratería		Pérdidas por piratería *(millones de dólares)*	
Venezuela	86%	Brasil	1.645
Paraguay	83%	México	823
Bolivia	81%	Venezuela	484
Guatemala	81%	Argentina	339
El Salvador	80%	Chile	202
R. Dominicana	79%	Colombia	136
Nicaragua	79%	Perú	84
Honduras	74%	Guatemala	49
Argentina	73%	R. Dominicana	43
Panamá	73%	Ecuador	37
Perú	71%	El Salvador	28
Uruguay	69%	Uruguay	25
Chile	67%	Costa Rica	24
Ecuador	66%	Panamá	24
Costa Rica	60%	Bolivia	20
México	59%	Paraguay	16
Brasil	58%	Honduras	9
Colombia	56%	Nicaragua	4

Fuente: Business Software Alliance